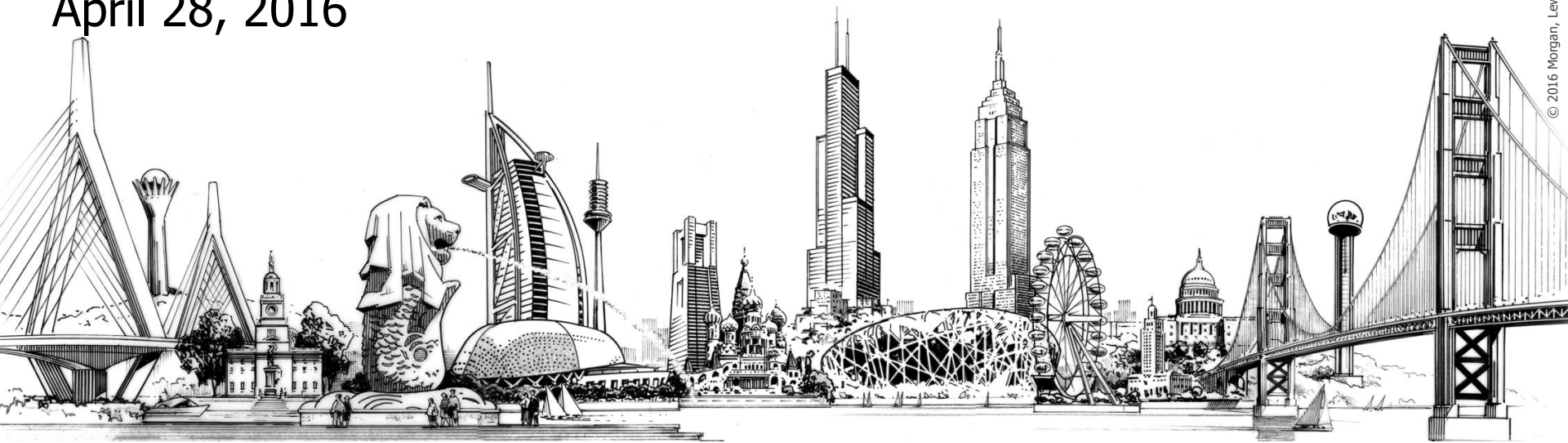
Morgan Lewis

PHASE 2: HIPAA PRIVACY AND SECURITY AUDITS

The ERISA Industry Committee

Sage Fattahian
April 28, 2016



Agenda

- Background / HIPAA Basics
- Pilot Program (Phase 1)
- Phase 2 Audits
- Next Steps

BACKGROUND / HIPAA BASICS

Applicability of HIPAA

- Covered Entity (exclusive list)
  - Health Plans
    - insurers and group health plans: medical, dental, prescription drug, employee assistance program, health care flexible spending account, certain long term care, wellness programs
  - Health Care Providers
    - that transmit health information in standardized e-format: physicians, other medical providers, hospitals, pharmacies
  - Health Care Clearinghouses
    - entities that convert data into or out of standardized e-format
- Business Associates (post HITECH)
  - third parties that perform services *for or on behalf of* the covered entity that involve the use, disclosure or maintenance of, or access to, PHI
  - third party administrators, billing services, attorneys, actuaries, consultants and accountants (*list is not exhaustive*)

HIPAA Privacy Rule and Security Rule

- **Privacy Rule**: Sets standards to limit how Protected Health Information ("PHI") is used and disclosed, and to provide individuals with certain rights related to their PHI

- **Security Rule**: Defines the administrative, physical and technical safeguards necessary to protect the confidentiality, integrity and availability of electronic PHI ("ePHI")

HITECH Impact

- HITECH was added under The American Recovery and Reinvestment Act of 2009
  - Amends Privacy and Security Rules
  - Establishes breach notification requirements
  - Establishes compliance requirements for Business Associates
  - Establishes increased penalty structure
  - Extends enforcement authority to States Attorney General
  - Requires HHS to provide for periodic audits to ensure compliance
    - To implement this mandate, OCR piloted a program to perform audits
    - Audits conducted in two phases

HIPAA Compliance Documents

- HIPAA Privacy Policies & Procedures
- HIPAA Security Policies & Procedures
- HIPAA Notice of Privacy Practice
- Business Associate Agreements
- Authorizations
- Group health plan language
- Document retention requirement

PILOT PROGRAM (PHASE 1)

OCR Audit Stated Objectives & Goals

- These are performance audits
- Not an enforcement action, though can be referred to enforcement
- Observations – compliance driven
- Examine mechanisms for compliance
- Identify best practices
- Discover risks and vulnerabilities that may have come to light through compliance investigations and compliance reviews
- Encourage renewed attention to compliance activities
- Objective: "To analyze the key processes, controls, and policies of the auditee relative to selected requirements of the Rules as specified in an OCR audit protocol and provide findings or observations."

Pilot Program Audits

- OCR conducted 115 performance audits in two phases:
  - Initial 20 audits
  - Final 95 audits
    - Of the 115 total performance audits 61 were providers, 47 were health plans and 7 were clearinghouses
- The objective of the performance audits:
  - To analyze the key processes controls and policies of the covered entity relative to the OCR audit protocol and provide findings or observations.
- Audit protocol: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol-current/index.html

Audit Timeline

- Timeline
  - Overall 30 – 90 business days broken up into four parts
- Part 1: Planning the Audit
  - Notification letter sent to covered entity and making contact
- Part 2: Preparation Work
  - Receiving and reviewing documents
- Part 3: Field Work
  - Conducting interviews, onsite visits, observing facilities/workstations
- Part 4: Post Field Work
  - Document results of audit
  - Finalize findings
  - Provide findings to covered entity for response
  - Issue final report

Phase 1 Results – Privacy Rule

- Privacy Rule Compliance Results
  - Most commonly :
    - Notice of Privacy Practice
      - Includes issues with content, website posting
    - Right to request privacy protections for PHI
    - Access of individuals to PHI
    - Administrative requirements
      - Training, policies & procedures, complaints, sanctions
    - Uses and disclosures of PHI
      - Business associate, identity verification, minimum necessary, authorizations, deceased individuals, personal representatives, judicial and administrative procedures, group health plan requirements

Phase 1 Results – Security Rule

- Security Rule Compliance Results
  - Deficiencies in compliance with the Security Rule accounted for 60% of the audit findings and observations
    - Most notably the lack of complete and accurate risk assessment in two-thirds of the entities audited
      - 47 of 59 providers
      - 20 of 35 health plans
      - 2 of 7 clearinghouses
    - 58 of 59 providers had at least one Security Rule finding or observation even though Security Rule audits represented 28% of the total audit items
- Covered entities that complied with the Security Rule fully implemented addressable specifications

Overall Results

- Most common cause for compliance failure was "entity unaware of requirement"
  - Privacy Rule – 39%
  - Security Rule – 27%
  - Breach Notification – 11%
- Other noted causes include:
  - Lack of application of sufficient resources
  - Incomplete implementation
  - Complete disregard

Overall Results

- "Entity unaware of requirement"
  - Privacy Rule
    - ❖ Notice of Privacy Practice
    - ❖ Access of individuals
    - ❖ Minimum necessary standard
    - ❖ Authorizations
  - Security Rule
    - ❖ Risk analysis
    - ❖ Media movement and disposal
    - ❖ Audit controls and monitoring
- Lessons Learned For Phase 2!!!!

HIPAA PHASE 2 AUDITS

When will audits begin

- Phase 2 currently underway
- Focus on covered entities and business associates
- OCR identifying audit pool (how?)
  - Communication sent via email
  - Spam – no excuse!
  - Sample email letter
    - ❖ 14 day response timeframe
    - ❖ Link in letter leads to online questionnaire
    - ❖ Failure to respond does not shield against audit

How will the audits be conducted

- OCR will conduct desk and onsite audits
- First set of audits will be desk audits
  - First round covered entities
  - Second round business associate
  - Examine compliance with specific requirements
  - Auditee will be notified of subject(s) of audit in a document request letter
  - All desk audits completed by end of December 2016
- Third round of audits will be onsite
  - Examine broader scope of HIPAA compliance
  - Some desk auditees may also be subject to onsite audit

What is the audit process

- Entities selected for an audit will receive an email notification
  - Asked to provide documents and other data
  - Documents submitted online via a new secure audit portal on OCR website
    - ❖ Within 10 business days
  - Auditor will share findings
  - Auditee shall have opportunity to respond to findings
    - ❖ Within 10 business days
  - All written auditee responses will be included in the final audit report
    - ❖ Within 30 business days
- Onsite audits expected to take 3 to 5 business days

NEXT STEPS

Next steps

- Ensure that OCR's emails are not being sent to junk or spam email box
- Prepare list of business associates
- Review compliance with substantive areas expected to be focus of Phase 2 audits
  - Periodically conducting HIPAA Security Rule risk analysis
  - Developing HIPAA policies and procedures
  - Developing breach notification procedures
  - Updated Notice of Privacy Practice
  - Encryption
  - Maintaining an inventory of information systems
  - Implementing a physical security plan for each location that maintains PHI
  - Providing timely access to PHI
  - Training

Next steps

- Identify your audit response team
- Consider self-audit

Biography

Sage Fattahian
Chicago
T +1.312.324.1744
F +1.312.324.1001
sage.fattahian@morganlewis.com

Sage Fattahian counsels clients on all aspects of health and welfare plans. She works with clients to comply with the complicated, shifting requirements under the Internal Revenue Code, ERISA, ACA, COBRA, and HIPAA. She also guides clients through the entire process of preparing and reviewing plan documents and related materials, as well as reviewing and negotiating services agreements with third parties.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing
Boston
Brussels
Chicago
Dallas
Dubai
Frankfurt
Hartford
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Santa Monica
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington

Morgan Lewis

THANK YOU